PTO/SB/21 (09-04)
Approved for use through 07/31/2009. OMB 0651-0031
U.S. Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE

Doc Code:

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

OIPE
APR 17 2006
IAP3
PATENT & TRADEMARK OFFICE

TRANSMITTAL FORM

(to be used for all correspondence after initial filing)

Total Number of Pages in This Submission: 10

Application Number	09/885,959
Filing Date	06/22/2001
First Named Inventor	GALLANT, Robert
Art Unit	2132
Examiner Name	LANIER, Benjamin E.
Attorney Docket Number	67539/00366

ENCLOSURES *(Check all that apply)*

- [ ] Fee Transmittal Form
- [ ] Fee Attached
- [x] Amendment / Reply
- [ ] After Final
- [ ] Affidavits/declaration(s)
- [ ] Extension of Time Request
- [ ] Express Abandonment Request
- [ ] Information Disclosure Statement
- [ ] Certified Copy of Priority Document(s)
- [ ] Response to Missing Parts/ Incomplete Application
- [ ] Reply to Missing Parts under 37 CFR 1.52 or 1.53
- [ ] Drawing(s)
- [ ] Licensing-related Papers
- [ ] Petition
- [ ] Petition to Convert to a Provisional Application
- [ ] Power of Attorney, Revocation Change of Correspondence Address
- [ ] Terminal Disclaimer
- [ ] Request for Refund
- [ ] CD, Number of CD(s) _____
  - [ ] Landscape Table on CD
- [ ] After Allowance Communication to TC
- [ ] Appeal Communication to Board of Appeals and Interferences
- [ ] Appeal Communication to TC (Appeal Notice, Brief, Reply Brief)
- [ ] Proprietary Information
- [ ] Status Letter
- [x] Other Enclosure(s) (please identify below):

1) copy of Notice of Abandonment in application no. 09/931,013; and
2) copy of Voluntary Amendment in application no. 11/095,542.

Remarks

SIGNATURE OF APPLICANT, ATTORNEY, OR AGENT

Firm Name	Blake, Cassels & Graydon LLP		
Signature			
Printed name	John R.S. Orange		
Date	April 17, 2006	Reg. No.	29,725

CERTIFICATE OF TRANSMISSION/MAILING

I hereby certify that this correspondence is being facsimile transmitted to the USPTO or deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria,VA 22313-1450 on the date shown below:

Signature			
Typed or printed name		Date	

This collection of information is required by 37 CFR 1.5. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

UNITED STATES PATENT AND TRADEMARK OFFICE

APR 17 2006
PATENT & TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/931,013	08/17/2001	Robert J. Lambert	06944.0037-01	2945

22852 7590 03/29/2006

FINNEGAN, HENDERSON, FARABOW, GARRETT & DUNNER LLP
901 NEW YORK AVENUE, NW
WASHINGTON, DC 20001-4413

EXAMINER	
CHAI, LONGBIT	

ART UNIT	PAPER NUMBER
2131	

DATE MAILED: 03/29/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

OIPE IAP
APR 17 2006
PATENT & TRADEMARK OFFICE

Notice of Abandonment	Application No. 09/931,013	Applicant(s) LAMBERT ET AL.	
	Examiner Longbit Chai	Art Unit 2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

This application is abandoned in view of:

1. ☒ Applicant's failure to timely file a proper reply to the Office letter mailed on 10/1/2004.
   (a) ☐ A reply was received on _____ (with a Certificate of Mailing or Transmission dated _____), which is after the expiration of the period for reply (including a total extension of time of _____ month(s)) which expired on _____.
   (b) ☐ A proposed reply was received on _____, but it does not constitute a proper reply under 37 CFR 1.113 (a) to the final rejection.
   (A proper reply under 37 CFR 1.113 to a final rejection consists only of: (1) a timely filed amendment which places the application in condition for allowance; (2) a timely filed Notice of Appeal (with appeal fee); or (3) a timely filed Request for Continued Examination (RCE) in compliance with 37 CFR 1.114).
   (c) ☐ A reply was received on _____ but it does not constitute a proper reply, or a bona fide attempt at a proper reply, to the non-final rejection. See 37 CFR 1.85(a) and 1.111. (See explanation in box 7 below).
   (d) ☒ No reply has been received.

2. ☐ Applicant's failure to timely pay the required issue fee and publication fee, if applicable, within the statutory period of three months from the mailing date of the Notice of Allowance (PTOL-85).
   (a) ☐ The issue fee and publication fee, if applicable, was received on _____ (with a Certificate of Mailing or Transmission dated _____), which is after the expiration of the statutory period for payment of the issue fee (and publication fee) set in the Notice of Allowance (PTOL-85).
   (b) ☐ The submitted fee of $_____ is insufficient. A balance of $_____ is due.
   The issue fee required by 37 CFR 1.18 is $_____. The publication fee, if required by 37 CFR 1.18(d), is $_____.
   (c) ☐ The issue fee and publication fee, if applicable, has not been received.

3. ☐ Applicant's failure to timely file corrected drawings as required by, and within the three-month period set in, the Notice of Allowability (PTO-37).
   (a) ☐ Proposed corrected drawings were received on _____ (with a Certificate of Mailing or Transmission dated _____), which is after the expiration of the period for reply.
   (b) ☐ No corrected drawings have been received.

4. ☐ The letter of express abandonment which is signed by the attorney or agent of record, the assignee of the entire interest, or all of the applicants.

5. ☐ The letter of express abandonment which is signed by an attorney or agent (acting in a representative capacity under 37 CFR 1.34(a)) upon the filing of a continuing application.

6. ☐ The decision by the Board of Patent Appeals and Interference rendered on _____ and because the period for seeking court review of the decision has expired and there are no allowed claims.

7. ☒ The reason(s) below:

Examiner called the attorney on record, Brett J. Slaney, and he said they abandoned it.

CHRISTOPHER REVAK
PRIMARY EXAMINER

3/26/06

Petitions to revive under 37 CFR 1.137(a) or (b), or requests to withdraw the holding of abandonment under 37 CFR 1.181, should be promptly filed to minimize any negative effects on patent term.

APR 17 2006

IN THE UNITED STATES PATENT & TRADEMARK OFFICE

Appl. No.: **11/095,542**

Applicant: **LAMBERT, Robert J. et al.**

Filed: **April 1, 2005**

Title: **Method For Accelerating Cryptographic Operations on Elliptic Curves**

Art Unit: **2131**

Examiner: **Not Yet Assigned**

Docket No.: **67539/00590**

Mail Stop Amendment
U.S. Patent & Trademark Office
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

VOLUNTARY AMENDMENT

Sir:

Prior to consideration by an Examiner, Applicant wishes to amend the above-identified application as follows:

Amendments to the Claims: are reflected in the listing of claims which begins on page 2 of this paper.

Remarks: begin on page 4 of this paper.

Amendments to the Claims

This listing of claims will replace all prior versions and listings of claims in the application:

Listing of claims:

1. – 16. (cancel)

17. (new) A method of calculating the sum of a plurality of point-multiples in a cryptographic scheme, said point multiples including the multiplication of respective scalars and respective points on an elliptic curve, said method comprising the steps of:

for each said plurality of point-multiples, computing a table of small multiples, said small multiples representing the multiplication of values smaller than said scalars and said points;

simultaneously windowing said scalars while reviewing corresponding bits of said scalars from a most significant bit thereof to a least significant bit thereof;

for each window encountered during said windowing, adding a corresponding one of said small multiples from its respective table to an accumulator; and

performing a doubling operation of said accumulator at each bit where the current bit from at least one of said scalars is zero.

18. (new) A method according to claim 17 wherein prior to said step of computing said tables, said method comprising the step of recoding said scalars from a binary representation to a signed binary representation.

19. (new) A method according to claim 18 wherein said signed binary representation is a Non-Adjacent Form (NAF).

20. (new) A method according to claim 17 wherein said windowing comprises one of a sliding window and a fixed window.

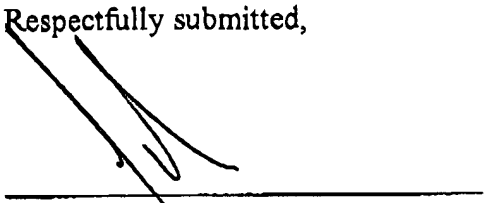
21. (new) A method according to claim 17 comprising a pair of point multiples in a signature verification scheme.

22. (new) A method according to claim 17 wherein the size of said tables is determined according to said windowing.

REMARKS

Claims 1-16 are cancelled and new claims 17-22 are added. Support for new claims 17-22 can be found in paragraphs [0084] to [0099] of the present application as published. No new subject matter is believed to have been added by way of these amendments.

Respectfully submitted,



John R.S. Orange
Agent for Applicant
Registration No. 29,725

Date: [illegible], 2006

BLAKE, CASSELS & GRAYDON LLP
Suite 2800, P.O. Box 25
199 Bay Street, Commerce Court West
Toronto, Ontario M5L 1A9
CANADA

Tel: 416.863.3164
JRO/BSL